The Performance Analysis of Post-Quantum Cryptography for Vehicular Communications

Abel C. H. Chen
Telecommunication Laboratories
Chunghwa Telecom Co., Ltd.
Taoyuan, Taiwan
ORCID 0000-0003-3628-3033

***Abstract*—For avoding the attacks from quantum computing (QC), this study applies the post-quantum cryptography (PQC) methods without hidden subgroups to the security of vehicular communications. Due the mainstream technologies of PQC methods (i.e. lattice-based cryptography methods), the standard digital signature methods including Dilithium and Falcon have been discussed and compared. This study uses a queueing model to analyze the performance of these standard digital signature methods for selection decision-making.**

***Index Terms*—Post-quantum cryptography, vehicular communications, queueing model, performance analysis**

I. Introduction

In the recent years, quantum computing (QC) has been more and more popular, and the quantum Fourier transform has been proposed to solve hidden subgroup problems by polynomial time computability. Furthermore, some cryptography methods (e.g. RSA (Rivest-Shamir-Adleman) and Elliptic Curve Cryptography (ECC)) including hidden subgroups may be cracked by QC. Therefore, the post-quantum cryptography (PQC) methods (e.g., lattice-based, multivariate-based, and code-based cryptography methods [1]) without hidden subgroups are important for defensing the attacks from QC.

For the security of vehicular communications, Security Credential Management System (SCMS) [2] and Cooperative Intelligent Transportation System Credential Management System (CCMS) have been designed based on Public Key Infrastructure (PKI). However, ECC is the used cryptography method in these systems, and security threats may be occurred by QC. Therefore, the PQC methods could be considered instead of ECC for improving the security levels.

In this study, the PQC methods that are applied to SCMS and CCMS will be surveyed and discussed. Furthermore, the lattice-based cryptography methods are the mainstream technologies of PQC methods [1]. Therefore, the performance of standard lattice-based cryptography methods (i.e. Dilithium and Falcon) will be compared. The main contributions of this study are listed as follows.

- This study implements standard lattice-based cryptography methods and measures the signature length and computation time of each method.
- This study uses the M/M/1 queueing model to analyze the average response time and the number of waiting packets for each standard lattice-based cryptography.

II. Measurement

This study implemented the methods of Dilithium [3] and Falcon [4] by C, Java, or Python languages for the digital signature of packets in SCMS and CCMS. The used machine includes Intel® Core™ i7-10510U and 8G RAM. The measured information including the signature length and computation time of each method is listed in Table I. The results show that Falcon has shorter signature lengths and Dilithium has shorter computation time. The detailed discussions are presented in the following subsections.

TABLE I
The Signature Length and Computation Time of Each Method

Method	**Language**	**Security Level**	**Signature Length (bytes)**	**Signature Time (ms)**	**Verifiaction Time (ms)**
Dilithium	C	Level 2	2,420	1.183	0.274
		Level 3	3,293	1.888	0.438
		Level 5	4,595	2.299	0.720
	Java	Level 2	2,420	**0.363**	**0.064**
		Level 3	3,293	**0.554**	**0.091**
		Level 5	4,595	**0.636**	**0.122**
Falcon	C	Level 1	**666**	6.896	0.190
		Level 5	**1,280**	13.804	0.358
	Python	Level 1	666	48.718	12.965
		Level 5	1,280	66.907	18.466

A. Signature Length and Transmission Time

According to the transmission rate of each communication protocol (e.g., IEEE 802.11p, IEEE 802.11bd, LTE-V2X, 5G NR-V2X, Zigbee, and LoRa [5]), the transmission time of signature by each PQC method could be estimated based on the signature lengths in Table I. For instance, the signature length of Dilithium based on Security Level 2 is 2,420 bytes, and the transmission time of the signature is 0.8 ms by the transmission rate of 23.08 Mbps through IEEE 802.11p (shown in Fig. 1). The results show that LTE-V2X and 5G NR-V2X have higher transmission rates for reducing transmission time. Furthermore, Falcon has shorter signature lengths, and the signature by Falcon could be transmitted faster.

B. Computation Time and Service Rate

For performance analysis, the service rates are considered in a M/M/1 queueing model. The service rates of signature and verification could be estimated based on the computation

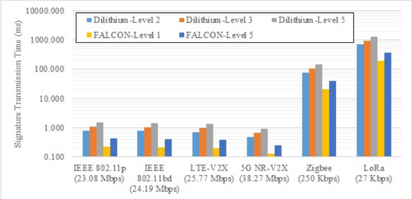

Fig. 1. The signature transmission time based on different communication techniques.

time of signature and verification in Table I. For instance, the computation time lengths of signature and verification by Dilithium based on Security Level 2 in C Language are 1.183 ms and 0.274 ms. Therefore, the service rates of signature and verification by Dilithium based on Security Level 2 in C Language could be estimated as 845.654 and 3,655.784 per second (shown in Table II). The results show that Dilithium in Java Language has short computation time, and the higher service rates could be obtained by Dilithium in Java Language.

TABLE II
The Service Rates of Signature and Verification

Method	Language	Security Level	Service Rate for Signature	Service Rate for Verification
Dilithium	C	Level 2	845.654	3,655.784
		Level 3	529.637	2,280.823
		Level 5	434.910	1,388.284
	Java	Level 2	**2,754.821**	**15,673.981**
		Level 3	**1,805.054**	**10,940.919**
		Level 5	**1,572.822**	**8,183.306**
Falcon	C	Level 1	145.004	5,265.375
		Level 5	72.443	2,796.264
	Python	Level 1	20.526	77.129
		Level 5	14.946	54.153

III. Numerical Analysis and Discussions

A M/M/1 queueing model is adopted according to the service rates in Subsection II.B and the arrival rates of packets from 1 to 14 for numerical analysis. Therefore, the average response time and the number waiting packets of signature by each PQC method could be estimated in Fig. 2 and 3. Furthermore, the average response time and the number waiting packets of verification by each PQC method could be estimated in Fig. 4 and 5. The results show that Dilithium in Java Language has higher performance and may be more suitable for vehicular communications with high-frequency signed transmission.

IV. Conclusions and Future Work

This study analyzed the performance of standard lattice-based cryptography methods (i.e. Dilithium and Falcon) for digital signature in vehicular communications. In numerical results, Dilithium in Java Language could obtain less waiting time and lower waiting packet number. Moreover, Falcon could be used for the case with shorter signature lengths. In the future, the more standard PQC methods in the fourth round by National Institute of Standards and Technology (NIST) [1] could be analyzed.

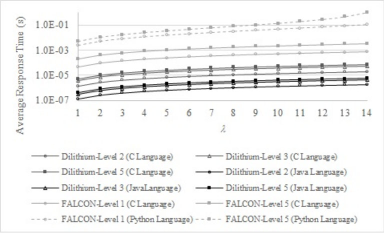

Fig. 2. The average response time of each PQC method for signature.

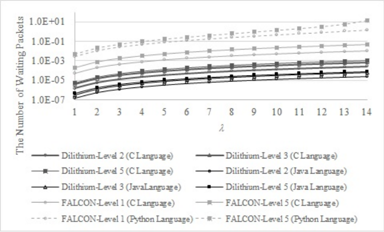

Fig. 3. The waiting packet number of each PQC method for signature.

References

[1] G. Alagic, D.A. Cooper, Q. Dang, T. Dang, J.M. Kelsey, J. Lichtinger, Y.K. Liu, C.A. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, D. Apon, "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process," NIST Interagency/Internal Report (NISTIR), National Institutes of Standards and Technology, Gaithersburg, MD, 2022.

[2] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, R. Goudy, "A Security Credential Management System for V2X Communications," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 12, pp. 3850-3871, 2018.

[3] "Dilithium." [Online]. Available: https://pq-crystals.org/dilithium/.

[4] "Falcon." [Online]. Available: https://falcon-sign.info/.

[5] W. Anwar, N. Franchi and G. Fettweis, "Physical Layer Evaluation of V2X Communications Technologies: 5G NR-V2X, LTE-V2X, IEEE 802.11bd, and IEEE 802.11p," 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), 2019, pp. 1–7.

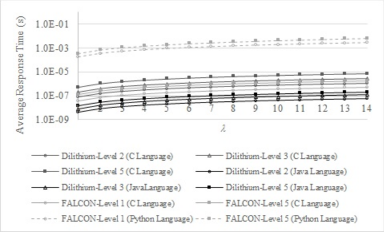

Fig. 4. The average response time of each PQC method for verification.

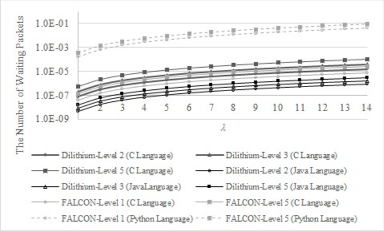

Fig. 5. The waiting packet number of each PQC method for verification.